Agenda

- Welcome
- Partnership Update
- Commonwealth of Virginia IT Security Program Overview
  - Information Technology Security Policy SEC500-02
  - Information Technology Security Standard SEC501-01
  - Information Technology Security Audit Standard SEC502-00
- Other Business
- Future meeting topics
- Questions & Answers

IT INFRASTRUCTURE PARTNERSHIP

Commonwealth Information Security Officers Meeting

Partnership Update

Presenter: Fred Duball

July 26, 2006

Virginia Information Technologies Agency

VITA

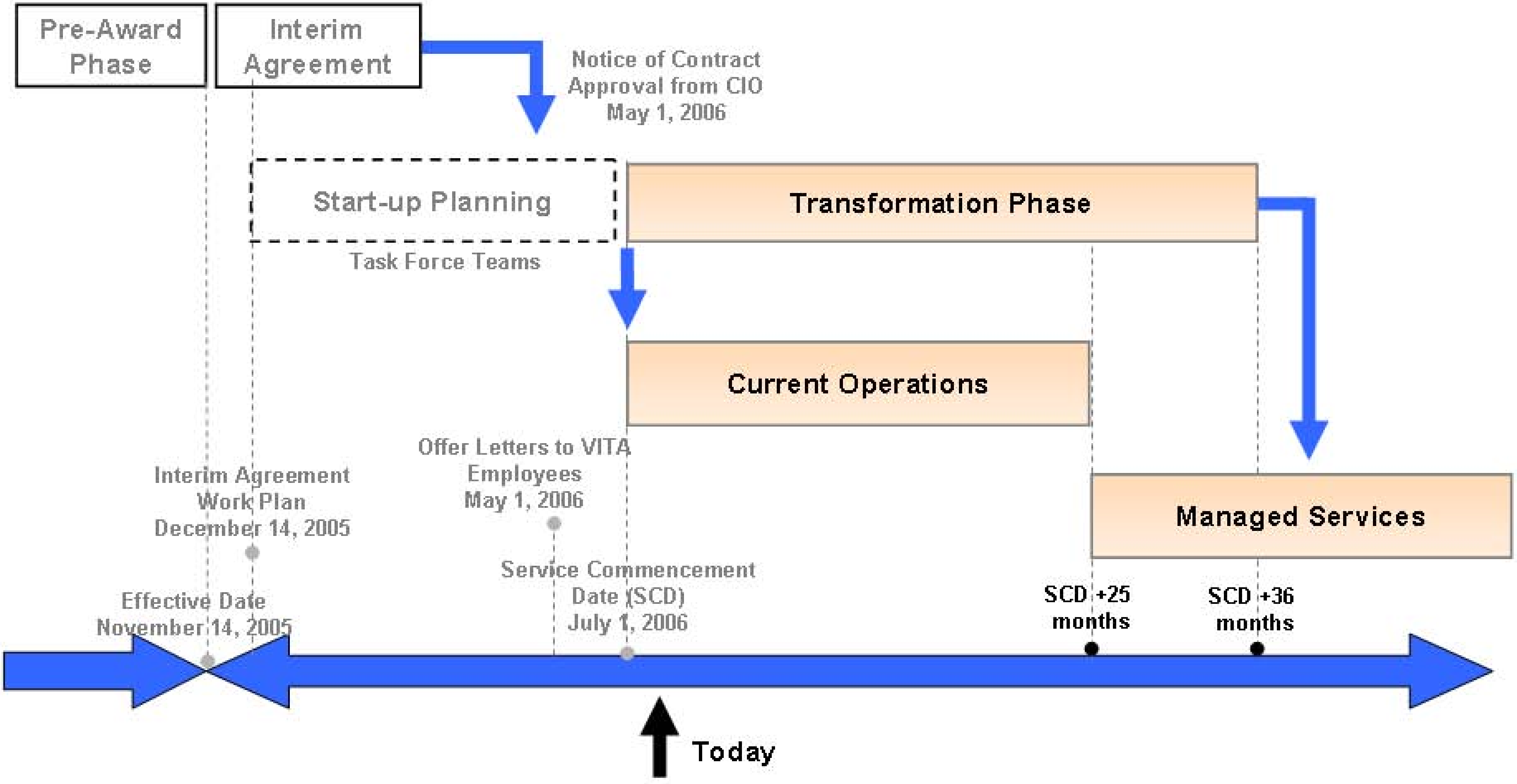
expect the best

NORTHROP GRUMMAN

Agenda

- Site Survey Team Activities
- Program Governance
  - Current Operations
  - Transformation
- Program-wide IV&V began June 19 with CACI

Implementation Timeline


Pre-Award Phase
Interim Agreement
Notice of Contract Approval from CIO May 1, 2006
Start-up Planning
Task Force Teams
Transformation Phase
Current Operations
Managed Services
Offer Letters to VITA Employees May 1, 2006
Interim Agreement Work Plan December 14, 2005
Service Commencement Date (SCD) July 1, 2006
Effective Date November 14, 2005
SCD +25 months
SCD +36 months
Today

Site Survey Teams

The IT future just got a little brighter in Virginia.
Here's to our new partnership.

State bird. State flower. State IT partner.

In Virginia, innovation and transformation are very much part of the picture. We at Northrop Grumman commend the Commonwealth for its forward-thinking views regarding the management of the States IT infrastructure needs. By having a big picture perspective, Virginia is bringing innovation and efficiency in State IT processes to the fore. A crucial point of view, we think, because thats exactly how Northrop Grumman has approached every project we've been involved with during our long-standing relationships with both state and local governments. And now, with our selection as the Commonwealth's IT infrastructure partner, we're honored to be offered this new opportunity to work with Virginia toward building a better, more effective IT infrastructure.

www.northropgrumman.com
©2005 Northrop Grumman Corporation

NORTHROP GRUMMAN
DEFENDING THE FUTURE

IT INFRASTRUCTURE PARTNERSHIP

Site Survey Team

- The Site Survey Team is designed to verify and collect physical data needed for Transformation.
- Expected to start in July 31, 2006 for pilot sites and late August for everyone else.
- Will run until January 31, 2007
- Order is still under development except for pilot sites.. Can’t do it too early or the data gets stale.

Site Survey Team

- Survey teams are comprised of 18 three person teams provided by SWAM partners.
- Team personnel have completed background checks to comply with Commonwealth standards for contractors.
- Minimal resource requirements at the agency. Escorted as needed by agency requirements.
- Pictures (where allowed) and other electronic data collection will be completed.
- Specific Security information and configurations to be collected by Central Security staff.

Site Survey Team

- Physical Review of Site
  - Photos, Access Points, Etc…
- Hardware Count
  - Desktop, Laptop, Printer, Servers
- Voice, Video, Telco Survey
  - Visual confirmation, Some Hardware Count

Program Governance

The IT future just got a little brighter in Virginia.
Here's to our new partnership.

State bird. State flower. State IT partner.

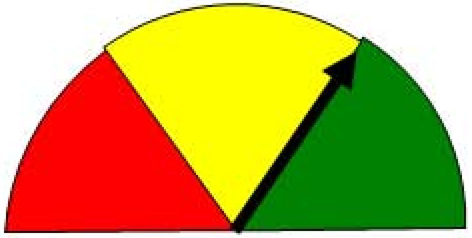
In Virginia, innovation and transformation are very much part of the picture. We at Northrop Grumman commend the Commonwealth for its forward-thinking views regarding the management of the States IT infrastructure needs. By having a big picture perspective, Virginia is bringing innovation and efficiency in State IT processes to the fore. A crucial point of view, we think, because thats exactly how Northrop Grumman has approached every project we've been involved with during our long-standing relationships with both state and local governments. And now, with our selection as the Commonwealth's IT infrastructure partner, we're honored to be offered this new opportunity to work with Virginia toward building a better, more effective IT infrastructure.

www.northropgrumman.com
©2005 Northrop Grumman Corporation

NORTHROP GRUMMAN
DEFINING THE FUTURE

IT INFRASTRUCTURE PARTNERSHIP

Program Vital Few Dashboard Week Ending 6/30/06 - *Closeout*



🟩 ***Employee Transition***	Executing to plan. Wave 1 onboarding complete.
🟩 ***Current Operations***	SCD-CC Operational. Final planning completed for SCD. Tracking SCD Punch List.
🟨 ***Critical Milestones*** ***Transformation***	3 projects in execution – working to finalize Initiation Phase artifacts
🟨 ***Financial Readiness***	Ongoing Contract Negotiations and Transition

Risk Description	**Potential Impact Description**	**Risk Mitigation Activities**
MOUII and Federal Funding approval	Partnership Budget	FMS pursuing Federal approval; Proceeding as if approval received

Issue Description	**Actual Impact Description**	**Resolution Activities**
VITA financial systems modifications	Limited VITA financial reporting	Aggressively tackling VITA system changes
On-Going Contract Negotiations and Transition	Assumed and Shared/Retained contracts need to be properly handled to support partnership objectives	VITA obtained access rights for July 1; NG focused on HW and Support. Both addressed Key Suppliers. Develop process and plan for executing contract disposition.

Evolving from Start-up and Interim to Current Operations and Transformation

- Vital Few
  - Employee Transition
  - Current Operations
  - Critical Milestones/ Transformation
  - Financial Readiness
- Joint Task Forces
  - SDM
  - Commercial Management
  - FMS-2B
  - Comms
  - Change
  - HR

- Transition Closeout
  - SCD Command Center & Punch List
  - Vital Few closure
  - Finance, Contracts, CIA
- Current Operations
  - End-User Services (EUS)
  - Data Center Services (DCS)
  - Network Services (NWS)
  - Security Services (SS)
- Transformation
  - EUS, DCS, NWS, SS

Elevating Overall IT Infrastructure Program View

- An end-to-end perspective of ITP's status and progress
  - Benefits Realization
    Value to various stakeholders, economic development, higher education partnerships and community outreach, etc.
  - Stakeholder Relationship Management
    Customer satisfaction and transformation readiness, effective internal and external communications, employee transition and development, supplier relationships, etc.
  - Governance
    Program & project management and controls, integration and interdependencies, budget and fiscal health, CIA management, IV&V, etc.

Current Operations

The IT future just got a little brighter in Virginia.
Here's to our new partnership.

State bird. State flower. State IT partner.

In Virginia, innovation and transformation are very much part of the picture. We at Northrop Grumman commend the Commonwealth for its forward-thinking views regarding the management of the States IT infrastructure needs. By having a big picture perspective, Virginia is bringing innovation and efficiency in State IT processes to the fore. A crucial point of view, we think, because thats exactly how Northrop Grumman has approached every project we've been involved with during our long-standing relationships with both state and local governments. And now, with our selection as the Commonwealth's IT infrastructure partner, we're honored to be offered this new opportunity to work with Virginia toward building a better, more effective IT infrastructure.

www.northropgrumman.com

NORTHROP GRUMMAN
DEFINING THE FUTURE

Infrastructure Service Areas Defined

End User Services (EUS)
Desktops: 68,457
Help Desks: 42
Messaging Systems: 48

Data Center Services (DCS)
Mainframes: 5
Servers: 3,287
Facilities

Network Services (NWS)
Circuits: 2876
Voice Networks/Circuits: 70,000
Video Bridges: 10

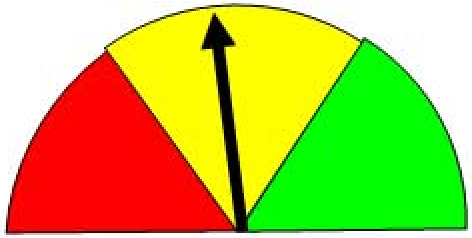
Security Services (SS)
VITA Central and Agency-based

To be validated during Data Collection exercises

VITA expect the best

NORTHROP GRUMMAN

Current Operations Dashboard



Quality of Service (QoS) Report (June)

EUS	🟩 3% Desktop 🟩 18% Messaging 🟨 36% Help Desk
DCS	🟩 Mainframe 100% 🟩 6% Servers
NWS	🟩 Communication – Data 90% 0% Communication - Voice
Security	🟩 60% Security

Note: Baselined percentages represent environment measured

Risk/Issue/ Incident	Impact	Resolution Activities
Issue: Unable to measure enterprise service levels against MOUs	Measure and monitor service delivery	Evaluate reasonable means to measure
Issue: Lack of request for service process	Delay in service requests and counter productive effort	Create and implement streamlined RFS process
Incident: Statewide outage at VDOT on 7/6/09	Workers could not access the network	Completed root cause analysis and implementing corrective action

Quality of Service (QoS) Summary

	Metrics Definition	Goal	Performance		
			Apr-06	May-06	Jun-06
EUS	Average Speed to Answer	<30 sec	26	27	32
	Call Abandon Rate	< 5%	5.63%	9.16%	5.41%
	Email Response	<60 mins	15	14	15
	Voicemail Response	<30 mins	14	14	15
	First Call Resolution	>70%	18%	23%	21%
	VITA Messaging System Availability	>99.0%	100%	100%	99.97%
	Shared Messaging System Availability	>99.0%	100%	99.99%	99.8%
DCS	IBM Mainframe Availability	>99.9%	100%	99.98%	99.95%
	Unisys Mainframe Availability	>99.9%	100%	100%	100%
	UNIX Server Availability	>99%	99.6%	99.95%	99.87%
	Windows Server Availability	>99%	99.6%	99.93%	99.98%
NWS	Circuits Availability*	>99.98%	99.3%	99.3%	n/a

* Measurement methodology being revised

Path to Automated SLA Reporting

Service Area	Interim Reporting Objectives	Service Levels (SLA)
End User Services (EUS)		
Help Desk Services	Jun-07	Jul-08
Messaging Services	Oct-07	Jun-09
Desktop Computing	Jun-07	Apr-09
Data Center Services (DCS)		
Mainframe & Server Services	Jun-07	Jun-09
Network Services (NWS)		
Data Network Services	May-07	Dec-08
Voice & Video Telecom	May-07	Jul-08
Security Services (SS)		
Security Services	May-07	Jun-09

Dates may be adjusted based on Annual Partnership Budgeting

Transformation

The IT future just got a little brighter in Virginia.
Here's to our new partnership.

State bird. State flower. State IT partner.

In Virginia, innovation and transformation are very much part of the picture. We at Northrop Grumman commend the Commonwealth for its forward-thinking views regarding the management of the States IT infrastructure needs. By having a big picture perspective, Virginia is bringing innovation and efficiency in State IT processes to the fore. A crucial point of view, we think, because thats exactly how Northrop Grumman has approached every project we've been involved with during our long-standing relationships with both state and local governments. And now, with our selection as the Commonwealth's IT infrastructure partner, we're honored to be offered this new opportunity to work with Virginia toward building a better, more effective IT infrastructure.

www.northropgrumman.com
©2005 Northrop Grumman Corporation

NORTHROP GRUMMAN
DEFINING THE FUTURE

Transformation Projects

End User Services (EUS)

Help Desk
Enterprise Help Desk in Lebanon and Meadowville
Field Based agents and technicians for Level 3
Enterprise Help Desk System (Peregrine)

Desktop
Mass Desktop Refresh Projects
Network Printer Consolidation and Refresh
Enterprise Desktop Management Systems

Messaging Services
Enterprise Exchange/Outlook Email
Enterprise Collaboration tools
Active Directory, DNS, DHCP

Data Center Services (DCS)

Mainframe and Servers
New IBM and Unisys Mainframes in new Data Center
Consolidation and refresh of servers
Migration of servers to the data center

Facilities
New Data Center/Office Building in Meadowville
New Disaster Recovery Center and Help Desk
in Lebanon/Russell County

Network Services (NWS)

Network
New Commonwealth wide MPLS Core WAN
LAN upgrades to local switches/routers as needed
Network Re-addressing of IP

Voice / Video
Voice over IP
Network optimized for voice and video traffic

Security Services (SS)

Security
Enterprise Security Operations Center
Computer Security Incident Response Center
Secure Internet Gateway

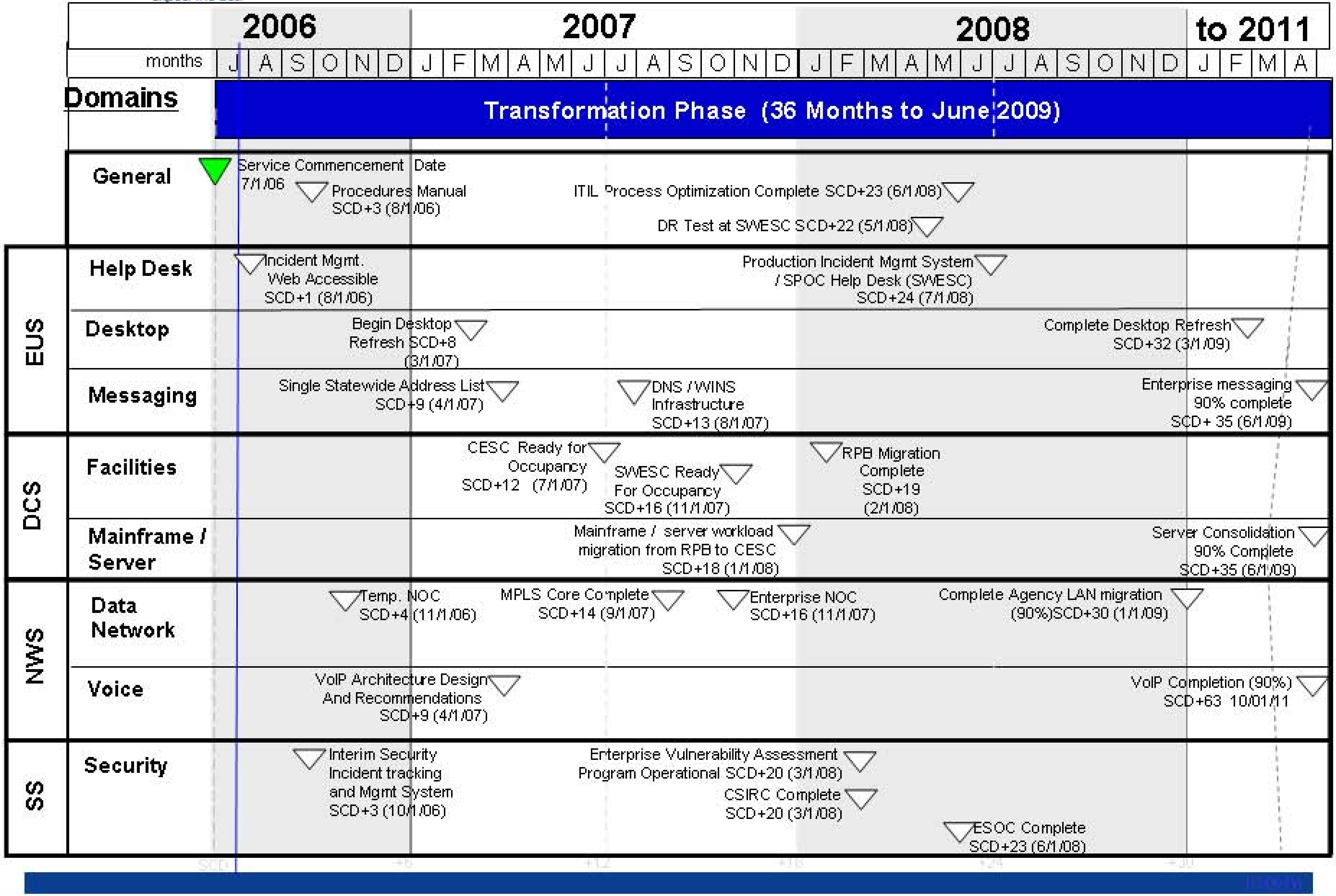
Transformation Launch Phase

- Data collection
  - Pilot data collection and inventory at 3 sites: July 2006
  - Incorporate lessons learned and process adjustments
  - Full data collection and inventory ~1,900 sites: Aug 2006 to Jan 2007
- Desktop & help desk transformation
  - Pilot agencies: Dec 2006 to Feb 2007
  - Review pilot results, include customer feedback and make modifications to transformation processes
  - Begin help desk deployment and refresh of 8,000 PCs per quarter March 2007 to April 2009
- Network deployment will follow
  - MPLS core complete Sept 2007

VITA expect the best

NORTHROP GRUMMAN

Transformation Schedule



Domains

Transformation Phase (36 Months to June 2009)

General

Service Commencement Date 7/1/06

Procedures Manual SCD+3 (8/1/06)

ITIL Process Optimization Complete SCD+23 (6/1/08)

DR Test at SWESC SCD+22 (5/1/08)

EUS

Help Desk

Incident Mgmt. Web Accessible SCD+1 (8/1/06)

Production Incident Mgmt System / SPOC Help Desk (SWESC) SCD+24 (7/1/08)

Desktop

Begin Desktop Refresh SCD+8 (3/1/07)

Complete Desktop Refresh SCD+32 (3/1/09)

Messaging

Single Statewide Address List SCD+9 (4/1/07)

DNS / WINS Infrastructure SCD+13 (8/1/07)

Enterprise messaging 90% complete SCD+ 35 (6/1/09)

DCS

Facilities

CESC Ready for Occupancy SCD+12 (7/1/07)

SWESC Ready For Occupancy SCD+16 (11/1/07)

RPB Migration Complete SCD+19 (2/1/08)

Mainframe / Server

Mainframe / server workload migration from RPB to CESC SCD+18 (1/1/08)

Server Consolidation 90% Complete SCD+35 (6/1/09)

NWS

Data Network

Temp. NOC SCD+4 (11/1/06)

MPLS Core Complete SCD+14 (9/1/07)

Enterprise NOC SCD+16 (11/1/07)

Complete Agency LAN migration (90%)SCD+30 (1/1/09)

Voice

VoIP Architecture Design And Recommendations SCD+9 (4/1/07)

VoIP Completion (90%) SCD+63 10/01/11

SS

Security

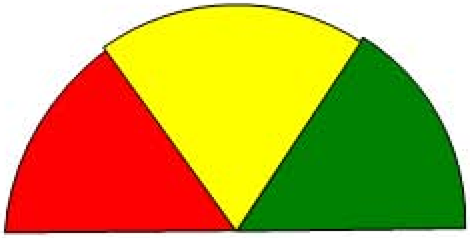
Interim Security Incident tracking and Mgmt System SCD+3 (10/1/06)

Enterprise Vulnerability Assessment Program Operational SCD+20 (3/1/08)

CSIRC Complete SCD+20 (3/1/08)

ESOC Complete SCD+23 (6/1/08)

Transformation Dashboard



EUS	Help Desk	Help Desk Peregrine web accessible on schedule for 8/1/06.
	Desktop	Planning being finalized.
	Messaging	
DCS	Facilities	CESC facility on schedule for 7/1/07 CO.
	Mainframe/Server	Planning being finalized.
	Cross Function	Procedures manual on schedule for 10/1/06.
NWS	Data Network	Planning being finalized.
	Voice Network	
SS	Security	Interim Security Incident tracking and Management system on schedule for 10/1/06.

Risk / Issue Description	Impact Description	Resolution Activities
Issue: Budget reduction will impact overall rollout schedule.	Specific impact unknown until all planning is completed	Complete budget review process. Re-solution transformation / rollout.
Risk: Agencies to be identified for the full transformation rollout plans.	Transformation and agency planning will delay meeting the scheduled rollout.	Develop a rolling 6 month look ahead schedule of agencies for deployment.
Risk: Network planning behind schedule	Delay in transformation rollout schedule	Leverage additional resources

Independent Verification & Validation

The IT future just got a little brighter in Virginia.
Here's to our new partnership.

State bird. State flower. State IT partner.

In Virginia, innovation and transformation are very much part of the picture. We at Northrop Grumman commend the Commonwealth for its forward-thinking views regarding the management of the States IT infrastructure needs. By having a big picture perspective, Virginia is bringing innovation and efficiency in State IT processes to the fore. A crucial point of view, we think, because thats exactly how Northrop Grumman has approached every project we've been involved with during our long-standing relationships with both state and local governments. And now, with our selection as the Commonwealth's IT infrastructure partner, we're honored to be offered this new opportunity to work with Virginia toward building a better, more effective IT infrastructure.

www.northropgrumman.com
©[illegible] Northrop Grumman Corporation

DEFINING THE FUTURE

Independent Verification and Validation (IV&V)

- Initial IV&V review of IT Infrastructure Partnership (ITP) program management practices began June 19 to be completed end of July
- Initial emphasis placed on development of an IV&V review framework compatible with the existing VITA PMD IV&V Program and suitable for use in future assessments
- Similar to the VITA PMD IV&V Program, the program management components of the ITP IV&V Framework are based upon the "best practices"
  - *PMBOK, 3rd Edition* as elevated to the program management level by PMI
  - *Organizational Project Management Maturity Model (OPM3)*
  - *Program Management Standard*

Independent Verification and Validation (IV&V)

- The operational (IT service management) components of the ITP IV&V Framework will be based upon ITIL

- The ITP IV&V Framework specifies the assessment of 39 Review Areas within 9 Practice Areas. The ITP IV&V Framework also specifies the accomplishment of 111 verification-level IV&V Tasks

- Personnel interviews began the last week of June and will continue through the end of this week

- Documentation reviews are ongoing

- The draft ITP IV&V Review Report is due 28 July

- Three quarterly ITP IV&V Reviews are scheduled to coincide with the next three ITIB meetings

VITA Virginia Information Technologies Agency

Commonwealth of Virginia Information Technology Security Program Overview

Peggy Ward
Chief Information Security and Internal Audit Officer

Scott Hammer
IT Security Consultant

Information Security Officers Advisory Group
July 26, 2006

expect the best

Agenda

- Introduction
- Commonwealth of Virginia (COV) IT Security Program Process Overview
- Questions and Answers

Goals of this Overview

- Assist you in protecting your Agency's IT assets and in understanding:
    - The documents that define COV IT security requirements and the interrelationship among these documents
    - COV IT security requirements
    - A recommended process for compliance
- Answer questions

COV IT Security Program Documents

- *IT Security Policy* (ITRM Policy SEC500-02)
  - Defines the overall COV IT security program
- *IT Security Standard* (ITRM Standard SEC501-01)
  - Describes high-level COV IT security requirements
- *IT Security Audit Standard* (ITRM Standard SEC507-00)
  - Describes COV IT Security Audit requirements

Purpose of the Policy and Standards

- Protect COV data against unauthorized access and use
- Maintain integrity of COV data
- Meet requirements for availability of data residing on IT systems
- Meet federal, state and other regulatory and legislative requirements
- Assess effectiveness of IT security controls

Policy and Standards Development

- IT Security Policy directions and the policy and standards documents were developed by a collaborative effort that involved input from a security workgroup comprised of:
  - Staff from VITA divisions including Security Services, and Policy, Practice and Architecture
  - Executive Branch Agency Information Security Officers (ISOs) including Institutions of Higher Education and staff from the Auditor of Public Accounts
  - Other Agencies via VITA's online review and comment application (ORCA)

Guiding Principles

- COV Data is:
  - A critical asset that shall be protected
  - Restricted to authorized personnel for official use
- IT security must be:
  - A cornerstone of maintaining public trust
  - Managed to address both business and technology requirements
  - Risk-based and cost-effective
  - Aligned with COV priorities, industry-prudent practices, and government requirements
  - Directed by policy but implemented by business owners
  - The responsibility of all users of COV IT systems and data

COV IT Security Program

- The COV IT Security Program consists of the following set of components:
  - Risk Management
  - IT Contingency Planning
  - IT Systems Security
  - Logical Access Control
  - Data Protection
  - Facilities Security
  - Personnel Security
  - Threat Management
  - IT Asset Management

COV IT Security Program

- The COV IT Security Program Provides:
  - A framework to allow COV Agencies to accomplish their missions in a safe and secure technology environment
  - A basis for each Agency's IT security program
    - Each component contains requirements that, together, comprise the COV IT Security Program
- Each Agency Head is accountable for protection of Agency IT systems and data

COV IT Security Program Roles

- The COV IT Security Program defines the following set of IT security roles:
  - Chief Information Officer of the Commonwealth (CIO)
  - Chief Information Security Officer (CISO)
  - Agency Head
  - Information Security Officer (ISO)
  - Privacy Officer
  - System Owner
  - Data Owner
  - System Administrator
  - Data Custodian
  - IT System Users

CIO

- In accordance with the *Code of Virginia* § 2.2-2009, the CIO:
  - *"Shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government databases and data communications. At a minimum, these policies, procedures, and standards shall address the scope of security audits and which public bodies are authorized to conduct security audits."*

CISO

- The CISO develops and coordinates the COV IT Security Program:
  - Administers the COV Security Program & periodically assesses whether it is implemented in accordance with COV IT Security Policies and Standards
  - Reviews requested exceptions to COV IT Security Policies, Standards, and Procedures
  - Provides solutions, guidance, and expertise in IT security
  - Maintains awareness of the security status of sensitive IT systems
  - Provides networking and liaison opportunities to Information Security Officers (ISOs)

Agency Head

- The Agency Head is responsible for the security of the Agency's IT systems and data:
  - Designates an ISO (and at least one backup) for the Agency and providing the person's contact information to VITA
  - Determines the place of the IT security function within the Agency hierarchy
  - Maintains an Agency IT security program to protect the IT systems
  - Reviews and approves the Agency's business impact analysis (BIA), risk assessment (RA), continuity of operations plan (COOP), and IT disaster recovery plan (DRP)
  - Establishes an IT security awareness and training program
  - Provides the resources necessary to secure IT systems and data

ISO

- The ISO is responsible for developing and managing an Agency IT security program that:
  - Meets or exceeds the requirements of COV IT security policies and standards
  - Develops and maintains IT security awareness and training for Agency staff, contractors, and IT service providers
  - Coordinates and provides IT security information to the CISO
  - Implements and maintains a balance of protective, detective, and corrective controls for IT systems commensurate with data sensitivity, risk, and systems criticality
  - Mitigates and reports all IT security incidents in accordance with the *Code of Virginia* and VITA requirements and takes appropriate actions to prevent recurrence

Privacy Officer

- An Agency must have a Privacy Officer if required by law or regulation, such as the Health Insurance Portability and Accountability Act (HIPAA), and may choose to have one where not required
- Otherwise, these responsibilities are carried out by the ISO
- The Privacy Officer provides guidance on:
  - Requirements of state and Federal Privacy laws
  - Disclosure of and access to sensitive data
  - Security and protection requirements in conjunction with IT systems when there is overlap among sensitivity, disclosure, privacy, and security issues

System Owner

- The System Owner is responsible for the operation and maintenance of an Agency IT system:
  - Requires that all IT system users complete security awareness and training prior to, or as soon as possible after, receiving access to the system
  - Manages system risk and develops security policies and procedures to protect the system
  - Maintains compliance with COV IT security policies and standards
  - Maintains compliance with requirements specified by Data Owners for the data processed by the system
  - Designates a System Administrator for the system

Data Owner

- The Data Owner is responsible for the policy and practice decisions of data:
  - Evaluates and classifies sensitivity of the data
  - Defines protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs
  - Communicates data protection requirements to the System Owner
  - Defines requirements for access to the data

System Administrator

- The System Administrator:
  - Implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner, and/or Data Custodian
  - Assists Agency management in the day-to-day administration of Agency IT systems
  - Implements security controls and other requirements of the IT Security Program on IT systems for which they are responsible

Data Custodian

- Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners and:
  - Protect the data in their possession from unauthorized access, alteration, destruction, or usage
  - Establish, monitors, and operates IT systems in a manner consistent with COV IT security policies and standards
  - Provide Data Owners with reports

IT System Users

- All users of COV IT systems (including employees and contractors) must:
  - Read and comply with Agency IT security program requirements
  - Report breaches of IT security, actual or suspected, to their agency management and/or the CISO
  - Take reasonable and prudent steps to protect the security of IT systems and data to which they have access

Agency Responsibilities

- The *IT Security Standard* defines the minimum acceptable IT security requirements for the COV
- Agencies must implement an IT security program in accordance with the *IT Security Standard*
- Agencies may implement their own IT security policies and standards, based on needs specific to their environments and commensurate with sensitivity and risk, as long as they provide protection equal to or greater than the requirements defined in the *IT Security Standard*

Agency Responsibilities

- Agencies may procure IT equipment, systems, and services from third parties
  - Agencies must enforce IT security compliance requirements through documented agreements with third-party providers
  - VITA customer Agencies must provide VITA with information concerning their IT security requirements to enable VITA to meet these requirements on their behalf

Applicability

- The requirements of the COV IT Security Program are applicable to all state Agencies and institutions of higher education that manage, develop, purchase, and use information technology resources
- The *Policy* and *Standards are* offered as guidance only to local government entities
- The *Policy* and *Standards* are not applicable to:
  - Systems under development and/or experimental systems that do not create additional risk to production systems
  - Surplus and retired systems
  - Academic instruction or research systems
    - This exemption, however, does not relieve these academic instruction or research systems from meeting the requirements of any other state or federal Law or Act to which they are subject

Requests for Exceptions

- If compliance with an IT security requirement would result in a significant adverse impact:
  - Agency Heads should submit a written exception request to the CISO (exception request form is in the Appendix of the *IT Security Policy* and *IT Security Standard)*
- Exception requests must document:
  - The business need
  - The scope and extent
  - Mitigating safeguards
  - The specific duration
  - Agency Head approval
- CISO evaluates and grants or denies requests for all exceptions
- Agencies may appeal denied exception requests to the CIO through the CISO

Organization of the *IT Security Policy*

- Defines the overall COV IT security policy and program:
  - **Key roles and responsibilities** of managers to provide IT security measures and controls to protect the COV IT systems and data
  - **Outline of IT security program components**, describing how each component fits into the overall IT security program
  - **Overview of IT security compliance** and proper administration of the COV IT Security Program with program management oversight
  - **Summary of IT security audit requirements** to test for adequacy of controls and assess compliance
  - **COV policy for the confiscation and removal of IT resources**
  - **Process for requesting an exception** to the requirements of this policy and the related standards

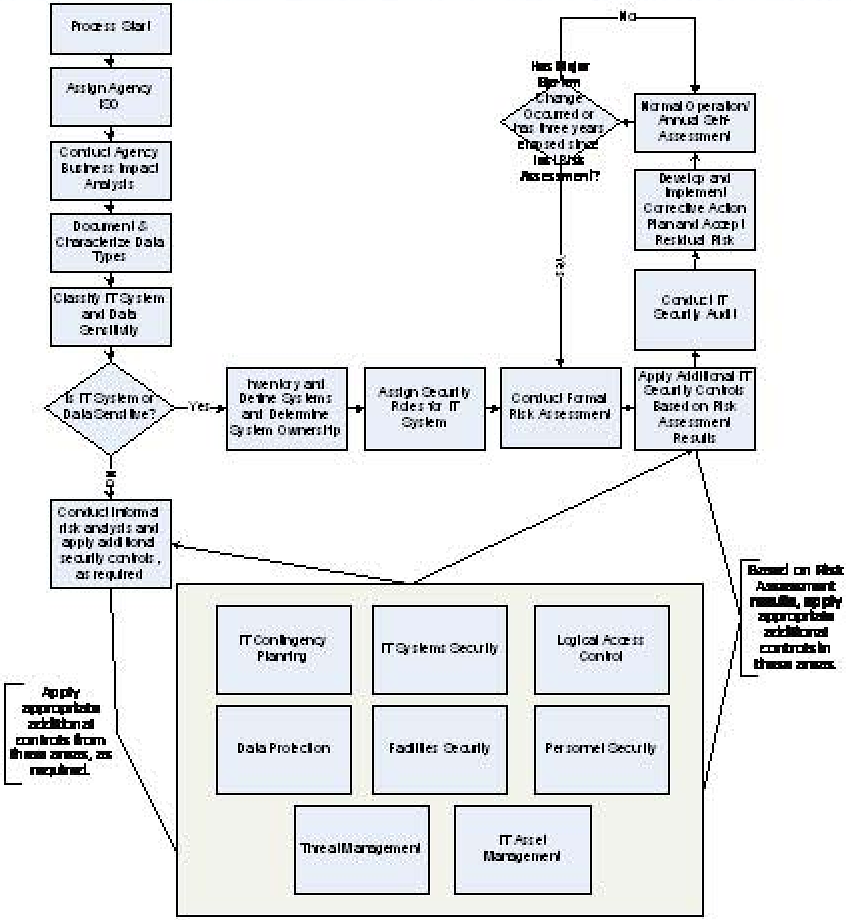
Organization of the *IT Security Standard*

- Organized around the nine components of the COV IT Security Program:
  - **Purpose statement**, that provides a high-level description of the component or subcomponent and its importance in the COV IT Security Program
  - **Requirements**, which describe mandatory technical or programmatic activities in detail for a specific area of the COV IT Security Program
  - **Notes**, which provide guidance and explanation regarding the requirements
  - **Examples**, which describe ways in which Agencies might meet the requirements
    - These examples do not and should not be interpreted to suggest an appropriate course of action for particular COV agencies, personnel, systems, or facilities

Organization of the *IT Security Audit Standard*

- The *IT Security Audit Standard* consists of:
  - **Definitions** of terms used in the document
  - **Requirements** for the planning, performance, and reporting of IT security audits

COV IT Security Program Process Flow



Process Start

Assign Agency ISO

Conduct Agency Business Impact Analysis

Document & Characterize Data Types

Classify IT System and Data Sensitivity

Is IT System or Data Sensitive?

Yes

No

Inventory and Define Systems and Determine System Ownership

Assign Security Roles for IT System

Conduct Formal Risk Assessment

Apply Additional IT Security Controls Based on Risk Assessment Results

Conduct IT Security Audit

Develop and Implement Corrective Action Plan and Accept Residual Risk

Normal Operation/ Annual Self-Assessment

Has Major System Change Occurred or has three years elapsed since last Risk Assessment?

No

Yes

Conduct Informal risk analysis and apply additional security controls, as required

Apply appropriate additional controls from these areas, as required.

Based on Risk Assessment results, apply appropriate additional controls in these areas.

IT Contingency Planning

IT Systems Security

Logical Access Control

Data Protection

Facilities Security

Personnel Security

Threat Management

IT Asset Management

COV IT Security Program Process Summary

For All Agency IT Systems:

- Assign Agency ISO
- Conduct Agency Business Impact Analysis
- Document and Characterize Types of Data
- Classify System and Data Sensitivity

For Non-Sensitive Agency IT Systems:

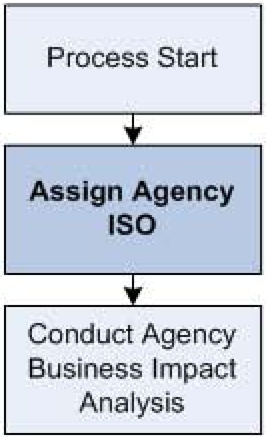
- Conduct informal Risk Analysis
- Apply additional IT security controls, as required

For Sensitive Agency IT Systems:

- Inventory and Define Systems and Determine System Ownership
- Assign Security Roles
- Conduct formal Risk Assessment and apply additional security controls based on results
- Conduct IT Security Audits
- Develop & implement Corrective Action Plan and accept residual risk
- Conduct annual self-assessment to validate that protections remain adequate
- Repeat Risk Assessment and Security Audit processes at least every three years or upon major change to the IT System

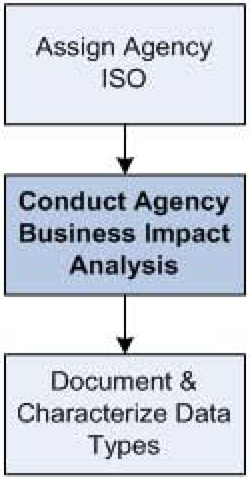
Assign Agency ISO

- The Agency ISO is responsible for developing and managing the Agency's IT security program
- Consequently, the first step in each Agency's process of implementing a security program must be formal assignment of the Agency ISO



Conduct Agency Business Impact Analysis

- Business Impact Analysis (BIA) requirements delineate the steps necessary for Agencies to:
  - Identify primary essential business functions
    - Identify secondary functions on which each essential function depends
  - Determine the required recovery time for each primary and secondary essential business function
  - Identify the resources that support each primary and secondary essential business function
    - For IT systems and/or data that support a primary or secondary essential business function, specify to what extent the essential business function depends upon the specific IT system and/or data
  - Produce a BIA report

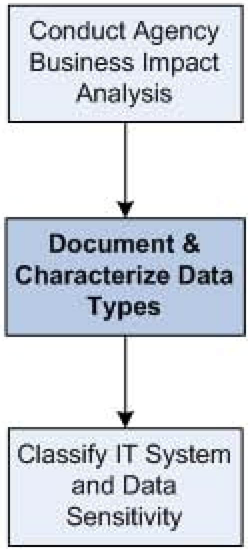

Assign Agency ISO

Conduct Agency Business Impact Analysis

Document & Characterize Data Types

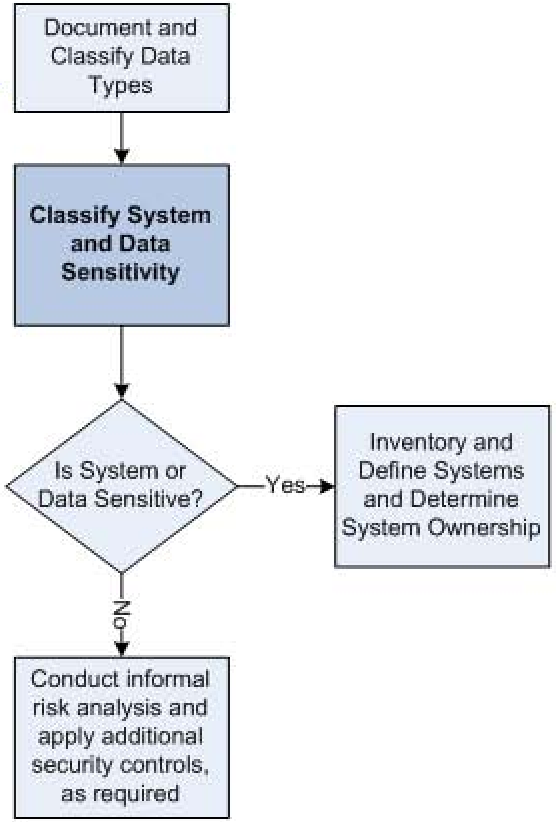
Document and Characterize Types of Data

- To provide IT security that is risk-based, cost-effective, and supports business needs, Agencies must prioritize protection of sensitive data
- Agencies need to have a comprehensive understanding of the types of data they collect, process, and store
- To develop this understanding, Agencies must document and characterize all the types of data they collect, process, and store


Conduct Agency Business Impact Analysis
Document & Characterize Data Types
Classify IT System and Data Sensitivity

Classify System and Data Sensitivity

- Sensitive Data is that which its compromise with respect to confidentiality, integrity, or availability (CIA) could adversely affect COV interests, the conduct of Agency programs, or individual privacy
- Sensitive IT Systems store, process, or transmit sensitive data
- Classify IT systems and data:
  - Identify the type(s) of data handled by each system
  - Classify the sensitivity of the data based on compromise of CIA:
    - **Confidentiality:** sensitivity to unauthorized disclosure
    - **Integrity:** sensitivity to unauthorized modification
    - **Availability:** sensitivity to outages


Document and Classify Data Types

Classify System and Data Sensitivity

Is System or Data Sensitive?

Yes

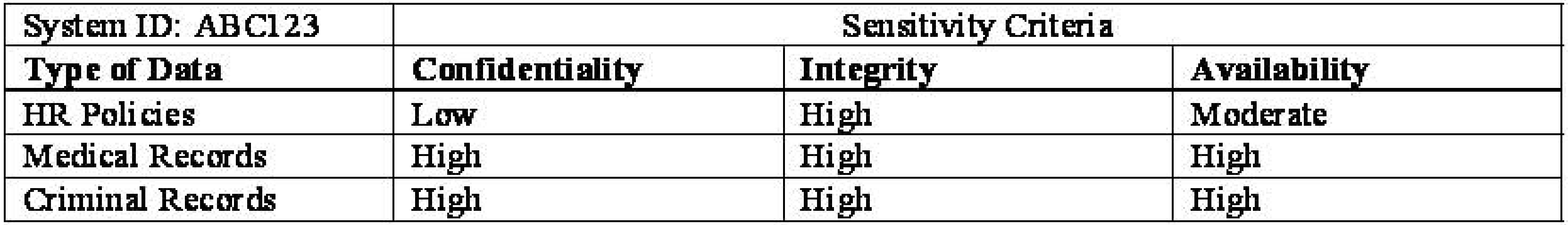
Inventory and Define Systems and Determine System Ownership

No

Conduct informal risk analysis and apply additional security controls, as required

Classify System and Data Sensitivity

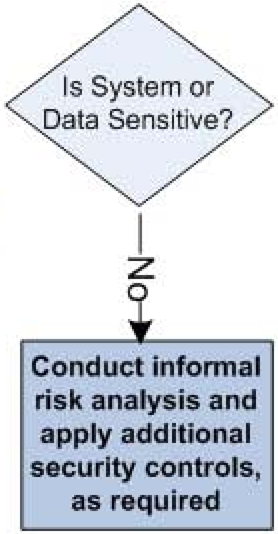
- Data Owners must classify sensitivity requirements of all types of data, and, to assist in this classification, Data Owners should construct a table similar to that below.
- Agencies must classify an IT system as sensitive if any type of data handled by the IT system has a sensitivity of high on any of the criteria of confidentiality, integrity, or availability
  - Agencies should consider classifying systems as sensitive even if a type of data handled by the IT system has a sensitivity of moderate on the criteria of confidentiality, integrity, and availability
- This sensitivity classification is a primary input to Risk Assessment



System ID: ABC123	Sensitivity Criteria		
Type of Data	**Confidentiality**	**Integrity**	**Availability**
HR Policies	Low	High	Moderate
Medical Records	High	High	High
Criminal Records	High	High	High

Informal Risk Analysis

- For each IT systems not classified as sensitive:
  - Conduct an informal risk analysis to identify significant threats to the IT system
  - Apply additional security controls, as required, based on the informal risk analysis, to protect against significant threats

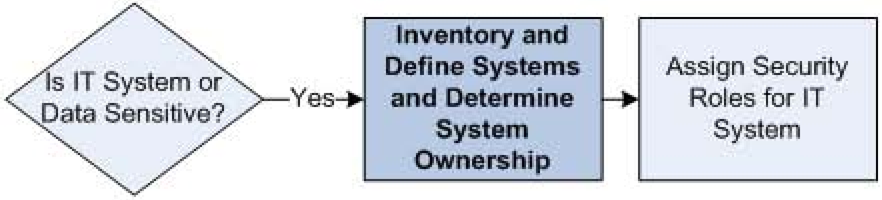

Is System or Data Sensitive?

No

Conduct informal risk analysis and apply additional security controls, as required

Inventory and Define Systems and Determine System Ownership

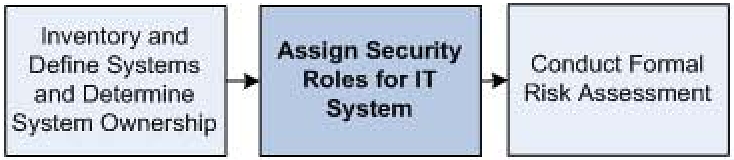
- Agencies must inventory and define and determine ownership of all Agency IT systems classified as sensitive so that IT security roles can be appropriately assigned
- Conduct an inventory of all sensitive IT systems owned by the Agency and update the inventory as changes occur
  - Document each IT system, including its boundary


Is IT System or Data Sensitive?
Yes
Inventory and Define Systems and Determine System Ownership
Assign Security Roles for IT System

Where more than one Agency may own the IT system, and the Agency or Agencies cannot reach consensus on which should serve as System Owner for IT security purposes, the CIO, upon request, will determine the System Owner

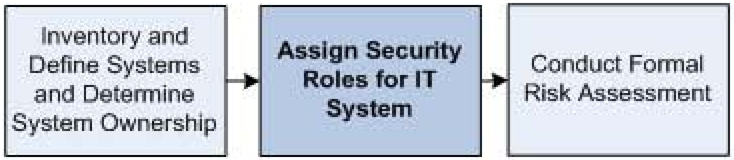
Assign Security Roles for Each Sensitive IT System

- For each Agency-owned IT system classified as sensitive, the Agency must assign a System Owner, Data Owner(s), and System Administrator(s)
  - A sensitive IT system may have multiple Data Owners, and/or System Administrators, but must have a single System Owner
    - The ISO must not be a System Owner
    - The System Owner and the Data Owner must not be System Administrator for IT systems or data they own
    - The ISO, System Owners, and Data Owners must be COV employees


Inventory and Define Systems and Determine System Ownership
Assign Security Roles for IT System
Conduct Formal Risk Assessment

Assign Security Roles for Each Sensitive IT System

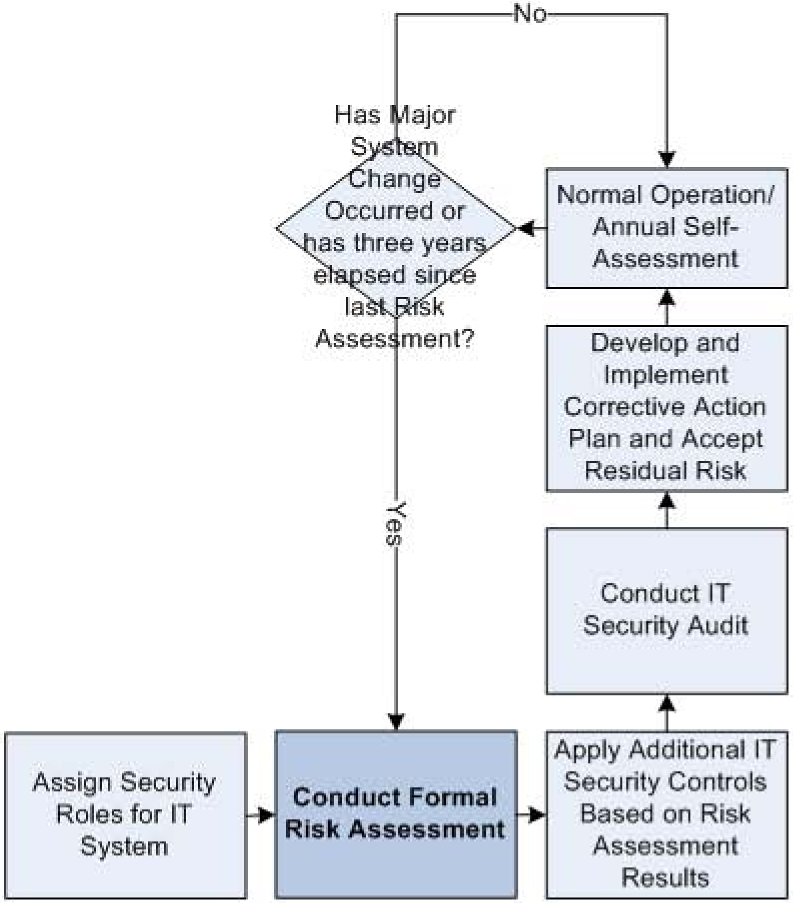
- IT security roles other than ISO, System Owner, and Data Owner may be assigned to contractors
  - For IT security roles assigned to contractors, the contract language must include specific responsibility and background check requirements
- System Owners may own multiple IT systems
- Data Owners may own data on multiple IT systems
- System Administrators may have responsibility for multiple IT systems



Inventory and Define Systems and Determine System Ownership → **Assign Security Roles for IT System** → Conduct Formal Risk Assessment

Conduct Formal Risk Assessment

- The RA process assesses the threats to Agency IT systems and data, probabilities of occurrence and the appropriate IT security controls necessary to reduce these risks to an acceptable level
- For each system classified as sensitive, Agencies must
  - Conduct a formal RA of the IT system not less than once every three years
  - Produce an RA report that includes:
    - Identification of all vulnerabilities discovered
    - An executive summary, including major findings and risk mitigation recommendations



Assign Security Roles for IT System

Conduct Formal Risk Assessment

Apply Additional IT Security Controls Based on Risk Assessment Results

Conduct IT Security Audit

Develop and Implement Corrective Action Plan and Accept Residual Risk

Normal Operation/ Annual Self-Assessment

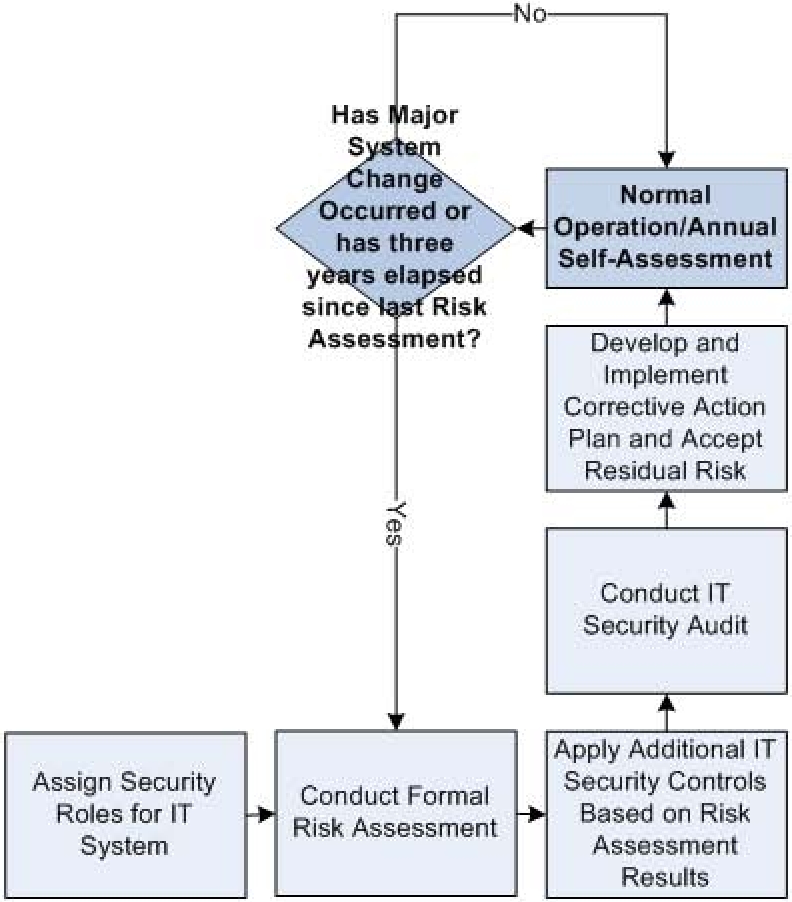
Has Major System Change Occurred or has three years elapsed since last Risk Assessment?

No

Yes

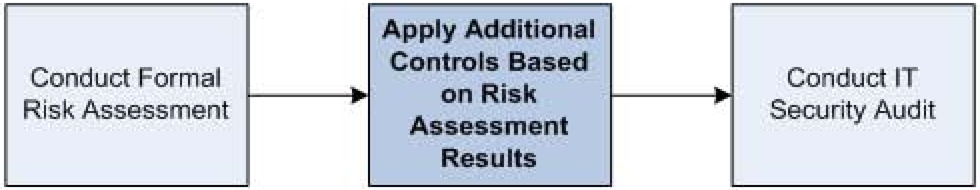
Annual Self Assessment

- Agencies must conduct an annual self-assessment that determines whether
  - IT security controls on the sensitive IT system remain adequate and effective
  - The IT system, its operating environment, or risks have changed sufficiently to require a new formal RA
- Formal RA must be repeated at least once every three years for each Agency-owned IT system classified as sensitive


No
Has Major System Change Occurred or has three years elapsed since last Risk Assessment?
Normal Operation/Annual Self-Assessment
Develop and Implement Corrective Action Plan and Accept Residual Risk
Yes
Conduct IT Security Audit
Assign Security Roles for IT System
Conduct Formal Risk Assessment
Apply Additional IT Security Controls Based on Risk Assessment Results

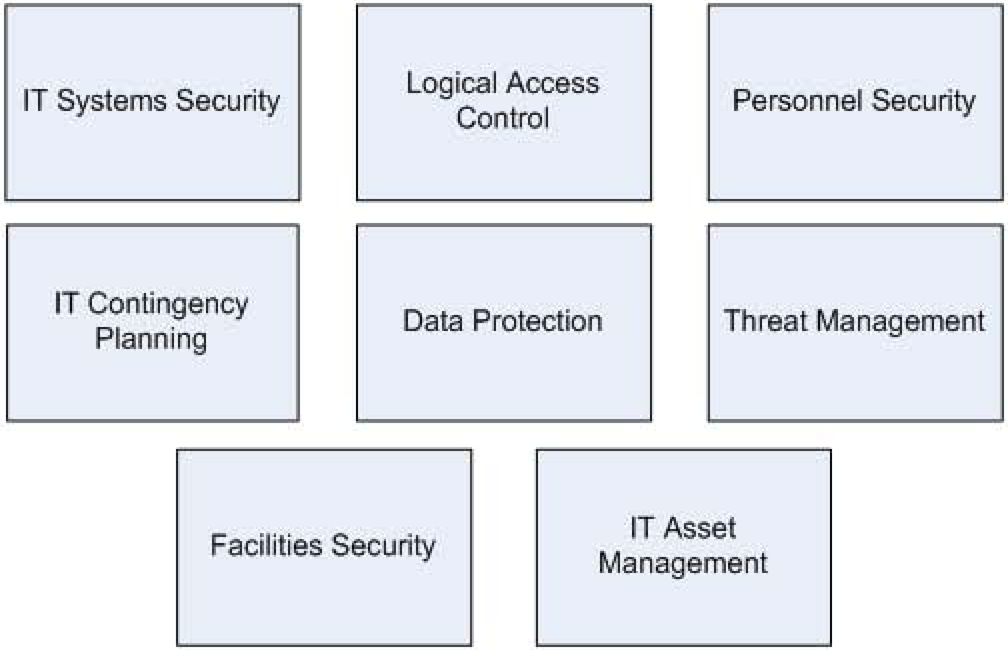
Application of Additional IT Security Controls

- Based on Risk Assessment results, additional security controls should be applied to protect against significant risks
  - This application of additional security controls is not a formal requirement of the COV IT Security Program, but a common-sense step to take after conducting a risk assessment and before conducting an IT security audit


Conduct Formal Risk Assessment
Apply Additional Controls Based on Risk Assessment Results
Conduct IT Security Audit

Additional Security Control Areas

- Application of additional security controls is a common means of protecting against risks discovered during Risk Assessment or Analysis
- Control areas include:
  - IT Contingency Planning
  - IT Systems Security
  - Logical Access Control
  - Data Protection
  - Facilities Security
  - Personnel Security
  - Threat Management
  - IT Asset Management



IT Systems Security

Logical Access Control

Personnel Security

IT Contingency Planning

Data Protection

Threat Management

Facilities Security

IT Asset Management

IT Contingency Planning

- IT Contingency Planning facilitates the recovery and restoration of IT systems and data if an event occurs that renders the systems and/or data unavailable
  - Continuity of Operations Planning
  - IT Disaster Recovery Planning
  - IT System Backup and Restoration

IT Contingency Planning

Continuity of Operations Planning

- VDEM defines continuity of operations planning (COOP) requirements that address all essential business functions
- The *Standard* addresses only the steps necessary to provide continuity for essential IT systems and data through the IT component of COOP:
  - Designate an employee to collaborate with the Agency COOP coordinator for IT aspects of COOP and Disaster Recovery planning activities
  - Based on BIA and RA results, develop COOP IT-related documentation identifying:
    - Essential business functions the Recovery Time Objective (RTO) for each
    - Recovery requirements for IT systems and data needed to support the essential business functions
    - Personnel contact information and incident notification procedures

IT Disaster Recovery Planning

- IT Disaster Recovery Planning is the component of COOP that identifies the steps to restore essential business functions on a schedule that supports Agency mission requirements
  - Develop and maintain an IT DRP which provides for restoring essential business functions
  - Periodically review, reassess, test, and revise DRP
  - Train all IT Disaster Recovery team members as part of the Agency's IT security training program
  - Establish communication methods to support IT system users' local and remote access to systems

IT System and Data Backup and Restoration

- IT System and Data Backup and Restoration requirements protect the availability and integrity of essential IT systems and data
- For every sensitive system, Agencies must implement backup and restoration plans to support recovery of systems and data:
  - Provide secure off-site storage for backup media
  - Review backup logs to verify successful completion
  - Develop system backup schedules, and emergency backup and operations restoration plans
  - Protect backup media that is sent off site (physically or electronically)

IT Systems Security

- IT Systems Security requirements delineate steps to protect IT systems in the following four areas:
  - IT System Hardening
  - IT Systems Interoperability Security
  - Malicious Code Protection
  - IT Systems Development Life Cycle

IT Systems Security

IT System Hardening

- System Hardening protects systems against security vulnerabilities
  - Apply appropriate baseline security configurations to IT systems, with more restrictive configurations for sensitive systems
  - Review and catalog security notifications issued by manufacturers, bulletin boards, and security-related Web sites; update security baseline configuration standards
  - Reapply all security configurations, as appropriate, if a system undergoes a material change, e.g. an operating system upgrade,
  - Periodically scan IT systems to verify whether security configurations are in place and functioning effectively; modify as needed

IT Systems Interoperability Security

- IT System Interoperability Security requirements identify steps to protect data shared with other IT systems
  - For each IT system classified as sensitive, the System Owner, in consultation with the Data Owner, must document IT systems with which data is shared. This documentation shall include:
    - Identifies the types of shared data
    - Identifies the direction(s) of data flow
    - Documents contact information for the organization that owns the IT system with which data is shared
  - System Owners develop a written agreement that defines IT security requirements for each interconnected IT system and for each type of data shared
  - System Owners inform one another regarding other systems with which their systems interconnect or share data, and prior to establishing any additional interconnections or data sharing

Malicious Code Protection

- Malicious Code Protection requirements protect IT systems from damage by malicious code
  - Prohibit all IT system users from knowingly developing, experimenting with, and propagating malicious programs, including opening e-mail attachments from unknown sources
  - Provide malicious program detection, protection, eradication, logging, and reporting capabilities
  - Provide training on malicious code protection best practices
  - Provide instructions for administrators and system users to counter malicious program attacks

Malicious Code Protection

- Malicious Code Protection requirements protect IT systems from damage by malicious code
  - Prohibit the installation of software on systems unless approved by ISO by written policy, and enforce this prohibition by automated means where possible
  - Provide malicious code protection mechanisms on multiple IT systems and for all IT system users preferably deploying malicious code detection products from multiple vendors on various platforms
  - By written policy, prohibit the installation of software on Agency IT systems until the software is approved by the Information Security Officer (ISO) or designee and, where practicable, enforce this prohibition using automated software controls, such as Active Directory security policies

IT Systems Development Life Cycle Security

- IT Systems Development Life Cycle Security requirements document the security-related activities that must occur in each phase of the development life cycle for IT application systems
  - Project Initiation
  - Project Definition
  - Implementation
  - Disposition

Logical Access Control

- Logical Access Control protects IT systems and data by verifying and validating that users:
  - Are who they say they are, and
  - Are permitted to use the systems and data they attempt to access

Logical Access Control

- This component defines requirements in the following three areas:
  - Account Management
  - Password Management
  - Remote Access

Account Management

- Document formal Account Management practices for requesting, granting, administering, and terminating accounts. At a minimum:
  - Define authentication and authorization requirements
  - Grant users access based on the principle of least privilege
  - Complete required background checks before establishing accounts, or as soon as possible thereafter
  - Provide for annual review of all user accounts for sensitive IT system to assess the continued need for the accounts and access level and periodic review of accounts on non-sensitive IT systems
  - Notify the System Administrator when user accounts are no longer required, or when an user's access level requirements change

Password Management

- Password Management practices require, for example:
  - Password use on all accounts on systems classified as sensitive
  - Use of passwords on mobile devices such as cellular telephones and Personal Digital Assistants (PDAs) based on sensitivity and risk
  - Users to maintain exclusive control and use of their passwords
  - Users to immediately change their passwords and notify the ISO if they suspect they have been compromised
  - At least two individuals with administrative accounts to each system

Remote Access

- Remote Access practices require, for example, that Agencies:
  - Protect the security of all remote access to the Agency's sensitive systems and data
  - Protect the security of remote file transfer of sensitive data to and from systems
  - Document requirements for use of remote access and to sensitive data
  - Document requirements for the physical and logical hardening of remote access devices

Data Protection

- Data Protection requirements delineate the steps necessary to protect data from improper or unauthorized disclosure
  - Data Storage Media Protection
  - Encryption

Data Protection

Data Storage Media Protection

- Data Storage Media Protection involves requirements for the appropriate handling of data to protect it from compromise, including:
  - Protection and identification of stored sensitive data is the responsibility of the creator or Data Custodian
  - Sensitive data must not be stored on mobile data storage media unless there is a documented Agency business necessity approved in writing by the Agency Head and unless all data storage media containing sensitive data are physically and logically secured
  - Storage media containing sensitive data are physically and logically secured
  - Restrictions to authorized personnel for the pickup, receipt, transfer, and delivery of storage media containing sensitive data
  - Storage media are sanitized prior to disposal or reuse

Encryption

- Encryption involves requirements to protect sensitive data from compromise, including:
  - Defining practices for selecting and deploying encryption technologies and for the encryption of data
  - Training users on the proper use of encryption products
  - Providing a secure key management system

Facilities Security

- Facilities Security requirements provide protection for the physical facilities that house IT equipment, systems, services, and personnel
  - Safeguard IT systems and data residing in static facilities, mobile facilities, and portable facilities
  - Design safeguards to protect against human, natural, and environmental risks
  - Require environmental controls such as electric power, heating, fire suppression, ventilation, air-conditioning and air purification
  - Provide a system of monitoring and auditing physical access to sensitive systems

Facilities Security

Personnel Security

- Personnel Security requirements restrict access to systems and data to those individuals who require such access as part of their job duties
  - Access Determination and Control
  - IT Security Awareness and Training
  - Acceptable Use

Personnel Security

Access Determination and Control

- Access Determination and Control requirements restrict access to systems and data to authorized individuals, by:
  - Performing background investigations of employees
  - Removing physical and logical access rights upon personnel transfer, termination, or when the need for access no longer exists
  - Establishing separation of duties or establishing compensating controls when not possible
  - Granting physical and logical access to sensitive systems and data and facilities based on the principle of least privilege

IT Security Awareness and Training

- Security Awareness and Training provides IT system managers, administrators, and users with awareness of system security requirements and of their responsibilities to protect systems and data
  - Designate an individual who is responsible for the Agency's security awareness and training program
  - Require that all employees and contractors receive IT security awareness training at least annually
  - Require security training before users receive access rights, or as soon as possible thereafter
  - Require documentation of system users' acceptance of the Agency's security policies after receiving training

Acceptable Use

- Acceptable Use requirements define acceptable and permitted use of IT systems
- Agencies must:
  - Adhere to Virginia Department of Human Resource Management Policy 1.75 – Use of Internet and Electronic Communication Systems
    - Each Agency shall supplement the policy as necessary to address specific agency needs

Acceptable Use

- Prevent users from:
  - Installing or using proprietary encryption hardware/software
  - Tampering with security controls configured on their workstations
  - Installing personal software
- Prohibit the use of copyrighted and licensed materials on systems unless owned or covered by intellectual property laws governing the materials
- Prohibit the transmission of unencrypted sensitive data over the Internet
- Document a system users' acceptance of the Agency's Acceptable Use Policy

Threat Management

- Threat Management delineates the steps necessary to protect IT systems and data by preparing for and responding to IT security incidents
  - Threat Detection
  - Incident Handling
  - Security Monitoring and Logging

Threat Management

Threat Detection

- Threat Detection requirements identify the practices for implementing intrusion detection and prevention, by:
  - Designating an individual responsible for the Agency's threat detection program
  - Requiring threat detection training for appropriate personnel
  - Developing and implementing mitigation measures based on the results of Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS) log reviews
  - Maintaining regular communication with security research and coordination organizations, such as US CERT

Incident Handling

- Incident Handling requirements identify the steps necessary to respond to suspected or known breaches to IT security safeguards, by:
  - Designating an Incident Response Team
  - Identifying controls to deter and defend against cyber attacks
  - Identifying immediate mitigation procedures
  - Establishing reporting of IT security incidents
  - Establishing procedures for incident investigation, preservation of evidence, and forensic analysis

Security Monitoring and Logging

- Security Monitoring and Logging requirements identify the steps necessary to monitor and record IT system activity, by:
  - Designating individuals responsible for monitoring logs
  - Enabling logging on all IT systems
  - Specifying the type of actions the program should take when a suspicious or apparent malicious activity is taking place
    - Possible actions include:
      - stopping the event
      - shutting down the system
      - alerting appropriate staff

IT Asset Management

- IT Asset Management delineates the steps necessary to protect systems and data by managing the IT assets in a planned, organized, and secure fashion
  - IT Asset Control
  - Software License Management
  - Configuration Management and Change Control

IT Asset Management

IT Asset Control

- Inventory Management requirements control and collect information about IT assets, by:
  - Identifying controls over removal of IT assets from premises that house IT systems and data
  - Identifying controls over allowing personal IT assets onto premises that house IT systems and data
  - Removing data from IT assets prior to disposal in accordance with the COV standard

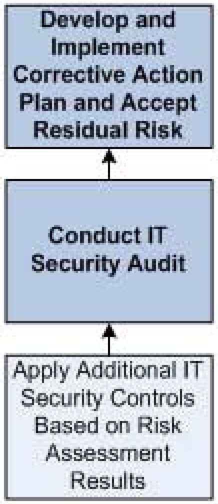
Software License Management

- Software License Management requirements protect against use of computer software in violation of applicable laws, by:
  - Requiring the use only of Agency approved software on COV IT systems
  - Periodically assessing whether all software is used in accordance with license agreements

Configuration Management and Change Control

- Configuration Management and Change Control requirements identify the steps necessary to document and monitor the configuration of IT systems, and to control changes during their lifecycles
  - Document configuration management and change control practices so that changes to the IT environment do not compromise IT security controls
  - Agencies are advised to institute practices based on industry standard frameworks such as the IT Infrastructure Library (ITIL) or Control Objectives for Information and related Technology (COBIT)

Conduct IT Security Audit



Develop and Implement Corrective Action Plan and Accept Residual Risk

Conduct IT Security Audit

Apply Additional IT Security Controls Based on Risk Assessment Results

IT Security Audit Standard

- The *IT Security Audit Standard* delineates the methodology for conducting IT security audits
- Agencies must conduct IT security audits of all Agency-owned IT systems at a frequency relative to risk
- At a minimum, all sensitive IT systems must undergo an IT security audit at least once every three years

Definitions

- **IT Security Audit**
  - An independent review and examination of an IT system's policies, records, and activities that assesses the adequacy of IT system controls and compliance with established IT security policy and procedures
- **IT Security Auditors**
  - Security Auditors have the experience and expertise required to perform IT security audits, including CISO personnel, Agency internal auditor, Auditor of Public Accounts, or staff of a private firm
- **Sensitive IT Systems and Data**
  - Sensitive Data is any data which the compromise of confidentiality, integrity, and/or availability could adversely affect COV interests, Agency programs, individual privacy rights
  - Sensitive IT Systems are that store, process, or transmit sensitive data

Security Audits of Government Databases

- The Agency's IT security audit program shall include:
  - Assessing the risks associated with the state government databases for which it is the Data Owner
  - Conducting IT Security Audits at a frequency relative to the risk identified by the Agency
- Assess at least once every three years those databases with sensitive data or reside in a system which has a sensitivity of high on any of the criteria of:
  - Confidentiality
  - Integrity, or
  - Availability (CIA)

Planning for IT Security Audits

- Agencies shall place reliance on audits already performed or underway
- Annually, each Agency shall develop an IT security audit plan for the government databases for which it is the Data Owner
- The IT security audit plan shall be based on the Agency's Business Impact Analysis (BIA) and Risk Assessment (RA)
- The Agency Head shall submit the Agency IT security audit plan to the CISO no later than 7 months after the effective date of this standard

Planning for IT Security Audits

- If a database relies upon IT services provided by VITA or any other service provider, the IT Security Auditor shall rely on any applicable IT Security Audits performed during the applicable audit cycle for that component of the IT Security Audit

- For IT services provided by VITA, the CISO will coordinate the VITA IT security audits

- If an Agency has VITA IT security audit needs that are not met through existing or planned IT security audits, the Agency should contact the CISO to address those needs

- It is the Agency's responsibility to ensure that adequate IT security audit provisions exist relative to other service providers

IT Security Audit Scope

- The IT Security Auditor shall use criteria that, at a minimum:
  - Measure compliance with the applicable requirements of:
    - ***Commonwealth of Virginia Information Technology Security Policy* (ITRM Policy SEC500-02)**
    - ***Commonwealth of Virginia Information Technology Security Standard* (ITRM Standard SEC501-01)**
  - Measure compliance with any other applicable Federal and COV regulations

Performance of IT Security Audits

- Prior to performing each IT Security Audit, the IT Security Auditor and the Agency Head or designee will agree on:
    - A specific scope
    - A schedule for the IT Security Audit
    - A checklist of information and access required for the Audit

Documentation of IT Security Audits

- IT Security Audit Work Papers
- IT Security Audit Reports
- Corrective Action Plan Reporting and Verification
- Reporting IT Security Audit Results to VITA

IT Security Audit Work Papers

- The Auditor shall prepare audit work papers to provide:
  - Documentation of the audit
  - Sufficient competent evidential matter supporting all conclusions
- The Auditor shall take care that:
  - Work papers do not constitute an unnecessary security risk
  - Are safeguarded appropriately

IT Security Audit Reports

- IT Security Auditor prepares a draft of the report for the Agency Head or designee and makes any mutually agreeable changes, then presents final IT Security Audit report to the Agency Head or designee
- Agency prepares a Corrective Action Plan (CAP) within 10 business days of receiving the final IT Security Audit report:
  - For each finding with which the Agency concurs, include the:
    - Corrective action planned
    - Due date for the corrective action
    - Party responsible for the corrective action
  - For each finding with which the Agency does not concur, include the:
    - Agency's statement of position
    - Mitigating controls that are in place
    - Agency's acknowledgment of its acceptance of the residual risk
- IT Security Auditor incorporates the CAP in the final Audit Report for presentation to the Agency Head and the Agency ISO

CAP Reporting and Verification

- Implementation
  - The Agency Head or designee shall receive reports, at least annually from the date of the final Audit Report, on progress in implementing outstanding corrective actions
- Verification
  - The Agency Head or designee shall arrange for a follow-up review to verify implementation of the specified corrective actions

Reporting IT Security Audit Results to VITA

- Each Agency Head or designee shall submit to the CISO a quarterly report containing:
  - A record of all IT Security Audits conducted and findings
  - Whether the Agency concurs or does not concur with each finding
  - The CAP for each finding with which the Agency concurs
  - The statement of position, mitigating controls, and risk acceptance for each finding with which the Agency does not concur
  - Status of outstanding corrective actions for all IT Security Audits previously conducted by or on behalf of the Agency

Additional Resources

- National Institute of Standards and Technology (http://www.nist.gov)
- Forthcoming Guidelines
  - Risk Management
  - Data Protection
  - Contingency Planning
  - Logical Access Control
  - IT Systems Security
  - Personnel Security
  - Threat Management
- FAQ on VITA website
- ISO Listserv
- VITASecurityServices@vita.virginia.gov

Questions and Answers

VITA Virginia Information Technologies Agency

Commonwealth of Virginia Incident Reporting Overview

Don Mills
CISSP CCNP CCDP
SCNA SCSA GCIA

Information Security Officers Advisory Group
July 26, 2006

expect the best

Incident Reporting

- Enacted by General Assembly as Code of Virginia § 2.2-603.F
- Calls for the director of every executive branch agency to report security incidents to the Commonwealth CIO within **24** hours of incident discovery
- http://www.vita.virginia.gov/security/incident/guidance.cfm

Advantages

- Provides timely threat information to Commonwealth Executive Management
- Allows for statistical trending and analysis of Commonwealth incidents
- Helps to correlate large scale (multi-agency) incidents
- Allows for appropriate activation of Commonwealth response teams (CIRT) to provide assistance

Commonwealth CIRT Team

- Group of security professionals trained in incident handling
- Wide variety of specialized technical skills in networking, Microsoft and Unix/Linux, databases, programming, forensics, etc.
- Can work incident from detection through resolution including interaction with law enforcement personnel
- Only of value if notified *during* incident as close to detection as possible

Incident Reporting and the Agency

- Definition of an incident
- What to report/not to report
- How to report

Definition of an Incident

- Incident: an adverse event, or series of events, in an information system, network, and/or workstation, or the threat of the occurrence of such an event
- Event: *any* observable occurrence in a system, network, and/or workstation. Although natural disasters and other non-security related disasters (power outages) are also called events, these reporting requirements are for IS security related events only. Events can many times indicate an incident is happening

What to Report

An "information security incident" should be reported if:

- it was intentional and successful AND
- it resulted in either:
  - a. unauthorized exposure or release of Commonwealth data held in Commonwealth or external databases;
  - b. major disruption to normal agency activities carried out via Commonwealth data communications, such as network unavailability for all or significant portions of an agency due to a denial of service (DOS) attack

What to Report Examples

- When damage is done
- Loss occurs
- Malicious code is implanted
- Evidence of tampering with data
- Unauthorized access or repeated attempts at unauthorized access (from either internal or external sources)
- Threat or harassment via electronic medium (internal or external)
- Access is achieved by the intruder
- Web pages are defaced
- When you detect something noteworthy or unusual (new traffic pattern, new type of malicious code, specific IP as source of persistent attacks).
- Denial of service attack on the agency
- Virus attacks which adversely affect servers or multiple workstations
- Other incidents that could undermine confidence and trust in the Commonwealth's information technology systems

What Not to Report

- Routine Probes and Scans
- SPAM unless it is a directed attack against your agency
- Viruses that are caught by Virus Protection systems
- Email attachments that are blocked
- BUT if in doubt, REPORT

How to Report

- Preferred method is via encrypted web form linked at http://www.vita.virginia.gov/security/incident/guidance.cfm
- Submittal to VCCC at 1-866-637-8482. Provide callback information for Security Services to contact you
- FAX completed offline form to 1-804-371-5235

Incident Reporting and VITA

- What happens to a report
- What VITA does with this information
- How VITA reports internal incidents with agency systems to the agency

What happens to a submitted report

- Incident Management receives real-time notification via email of the submittal with the submitted information
- Incident Management contacts the submitter to gather information and confirm the incident
- Incident Management notifies VITA executives that a confirmed incident has occurred, and mobilizes the CIRT team if appropriate

What VITA does with submitted data

Collected information from submitted reports is stored for statistical analysis by Incident Management engineers. Otherwise the information remains confidential.

VITA notification of Agency policy

For incidents that are reported internally on agency systems by VITA staff the following policy applies:

- VITA staff report incidents via the same web-based form
- Internally reported incidents follow same procedure as externally reported incidents with one exception
- Exception is that as soon as the incident is confirmed, the Agency ISO, AITR, and VITA Regional Service Director are notified

Questions and Answers